



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/072,663	02/07/2002	Dongfeng Jing	08212/000S007-US0	3310
38879	7590	04/10/2006	EXAMINER	
<b>DARBY &amp; DARBY P.C.</b> P.O. BOX 5257 NEW YORK, NY 10150-6257				POWERS, WILLIAM S
		ART UNIT		PAPER NUMBER
				2134

DATE MAILED: 04/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)	
	10/072,663	JING ET AL.	
	Examiner William S. Powers	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 19 January 2006.  
 2a) This action is **FINAL**.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-20 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) 1-12 is/are allowed.  
 6) Claim(s) 13-20 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 19 January 2006 is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
 Paper No(s)/Mail Date \_\_\_\_\_.  
 4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date \_\_\_\_\_.  
 5) Notice of Informal Patent Application (PTO-152)  
 6) Other: \_\_\_\_\_.

**DETAILED ACTION**

***Response to Amendment***

In light of Applicant's amendments, prior objections to the specification are withdrawn.

In light of Applicant's amendments, prior objections to claims 1, 3, 5 and 8 are withdrawn.

In light of Applicant's amendments, prior rejections to claims 1-12 under 35 USC 112, 2<sup>nd</sup> paragraph are withdrawn.

In light of Applicant's amendments, prior rejections to claims 1-12 under 35 USC 103(a) are withdrawn.

***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148

USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Application No. 2001/0016492 to Igarashi et al. (hereinafter Igarashi) in view of US Patent Application No. 2002/0118674 to Faccin et al. (hereinafter Faccin) in further view of US Patent No. 6,922,404 to Narayanan et al. (hereinafter Narayanan).

As to claim 13, Igarashi teaches:

- a. An MN, an AAAH, an AAAF, an HA, and an FA that are part of a communication network (page 11, paragraphs 227-230).
- b. Securing a Reg-Req message and a Reg-Reply message used in establishing the secure associations (page 11, paragraphs 227-230).

Igarashi teaches the use of security protocols and measures (page 9, paragraph 196), but does not expressly mention the use of security associations between the various nodes. However, in an analogous art, Faccin teaches establishing secure associations to help ensure secure communications within the network (page 2, paragraphs 29-page 3, paragraph 31).

c. Faccin further teaches distributing the session keys in a secure manner (page 3, paragraphs 36-41).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the AAA protocol for an IP network of Igarashi with the security associations and session key of Faccin in order to exchange information in a secure, authenticated manner and derive said session key as suggested by Faccin (abstract).

Although Igarashi and Faccin teach the use of a session key within their respective inventions, neither one expressly mentions creating a plurality of session keys. However, in an analogous art, Narayanan teaches creating a plurality of session keys by the AAAH and the AAAF (column 4, lines 41-60).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the AAA protocol for an IP network with security associations and session keys of Igarashi and Faccin with the multiple session keys of Narayanan in order to establish security associations between different entities as suggested by Narayanan (column 4, lines 49-51).

As to claim 14, Igarashi, as modified above, teaches using a home authority and a foreign authority to maintain and help establish the secure associations (Faccin, page 2, paragraph 30-page 3, paragraph 31).

As to claim 15, Igarashi, as modified above, teaches:

- a. Establishing a secure association between the MN and the AAAH (Faccin, page 2, paragraph 21).
- b. Establishing a secure association between the AAAH and the HA (Faccin, pages 3-4, paragraph 42).
- c. Establishing a secure association between the AAAF and the AAAH (Faccin, page 2, paragraph 29).
- d. Establishing a secure association between the AAAF and the FA (Faccin, pages 3-4, paragraph 42).
- e. Establishing a secure association between the AAAF and the MN (Faccin, page 3, paragraph 39).

As to claim 16, Igarashi, as modified above, teaches determining when a signature is an authentic signature based on the secure associations and the session keys (using derived public keys and sessions keys to ensure the validity of the messages passed within the network) (Faccin, page 4, paragraph 44).

As to claim 17, Igarashi, as modified above, teaches signing the Reg-Req message and the Reg-Reply message using the session keys; and authenticating the received Reg-Req message and the Reg-Reply message (the use of security associations and the respective session keys to transmit, authenticate and authorize messages and keys in a secure manner between nodes) (page 2, paragraph 30-page 3, paragraph 31).

As to claim 18, Igarashi, as modified above, teaches creating the session keys further comprises utilizing Diffie-Hellman parameters and the Diffie-Hellman algorithm (Faccin, page 2, paragraphs 23-28).

As to claim 19, Igarashi, as modified above, teaches that the Reg-Req message includes an NAI associated with the MN (Igarashi, page 8, paragraphs 175-177), a timestamp (lifetime of service profile) (Igarashi, pages 20-21, paragraph 456), a challenge issued by the FA (Faccin, page 3, paragraph 42), and the Diffie-Hellman parameters (Faccin, page 2, paragraphs 23-28).

As to claim 20, Igarashi, as modified above, teaches the Reg-Reply message includes an identifier and the session keys (Igarashi, page 5, paragraph 131).

### ***Response to Arguments***

4. Applicant's arguments, see page 11, line 25-page 12, lines 1-2, filed 1/19/2006, with respect to the rejection(s) of claim(s) 1-12 under 35 USC 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of newly found prior art, US Patent No. 6,922,404 to Narayanan et al. (hereinafter Narayanan). Narayanan teaches the use of multiple session keys to create secure

communication triangle between the mobile node and the home agent, mobile node and the foreign agent and the foreign agent and the home agent (column 4, lines 27-60).

***Allowable Subject Matter***

5. The following is a statement of reasons for the indication of allowable subject matter: the limitation in claim 1 that "an AAAH that is configured to: ... generate a second at least one key of the session keys ... generate a third at least one key of the session keys." The closest prior art found by the Examiner is Narayanan who teaches the use of multiple session keys, but does not expressly mention that the AAAH generates two of those session keys.

***Conclusion***

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to William S. Powers whose telephone number is 751 272 8573. The examiner can normally be reached on m-f 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on 571 272 6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
William S. Powers  
Examiner  
Art Unit 2134

  
Jacques H. Louis-Jacques  
PRIMARY EXAMINER